ELECTRONIC WATERMARK COMPOSITING DEVICE AND IMAGE ALTERATION DECIDING DEVICE

Patent Number: JP2001078013
Publication date: 2001-03-23
Inventor(s): ARAGAI YASUHIRO; TAKENAKA YUJI
Applicant(s): FUJI PHOTO FILM CO LTD
Requested Patent: JP2001078013
Application Number: JP19990250297 19990903
Priority Number(s):
IPC Classification: H04N1/387; G06T1/00; G09C1/00; G09C5/00; H04L9/32
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To composite an electronic watermark with an image photographed by an order receiver based on the request of an orderer by compositing cipher information which is prepared by enciphering image identification information for identifying an input image with the image as an electronic watermark, recording it and reporting a method thereof and the image identification information.
SOLUTION: A method for extracting the electronic watermark composited with an image 10, a method for deciphering the cipher information to be used as electronic watermark and the image identification information of the image 10 to be used for preparing the cipher information are reported by the manager of a laboratory system to the user of an image alteration discriminating device 90, namely, to the orderer. The order receiver receives a recording medium such as CD-ROM storing a composited image 11 from a laboratory system, selects a required image out of recorded images and presents it to the orderer as photograph data for proving progress. In order to discriminate whether an image 12 presented by the order receiver is altered, the orderer uses the image alteration discriminating device 90.

(19)日本国特許庁(JP)　　(12)公開特許公報（Ａ）　　(11)特許出願公開番号

特開２００１－７８０１３

(Ｐ２００１－７８０１３Ａ)

(43)公開日　平成13年3月23日(2001.3.23)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｈ０４Ｎ	1/387		Ｈ０４Ｎ	1/387		5B057
Ｇ０６Ｔ	1/00		Ｇ０９Ｃ	1/00	６４０　Ｂ	5C076
Ｇ０９Ｃ	1/00	６４０			６４０　Ｄ	5J104
				5/00		
	5/00		Ｇ０６Ｆ	15/66	Ｂ	

審査請求　未請求　請求項の数１１　ＯＬ　（全１０頁）　最終頁に続く

(21)出願番号　特願平11-250297

(22)出願日　平成11年9月3日(1999.9.3)

(71)出願人　000005201
富士写真フイルム株式会社
神奈川県南足柄市中沼210番地

(72)発明者　新貝　安浩
東京都港区西麻布2丁目26番30号　富士写真フイルム株式会社内

(72)発明者　竹中　裕二
東京都港区西麻布2丁目26番30号　富士写真フイルム株式会社内

(74)代理人　100104156
弁理士　龍華　明裕

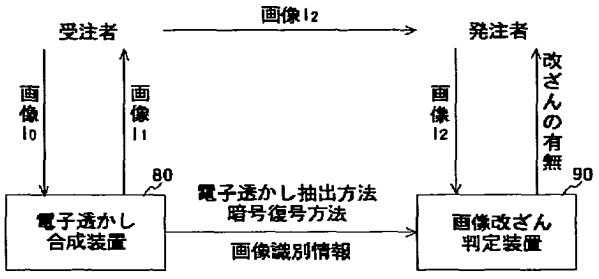
最終頁に続く

(54)【発明の名称】電子透かし合成装置及び画像改ざん判定装置

(57)【要約】

【課題】　画像に電子透かしを合成する画像合成装置、及び画像の改ざんの有無を判定する画像改ざん判定装置を提供する。

【解決手段】　画像を入力する画像入力部と、画像を識別する画像識別情報を暗号化した暗号情報を作成する暗号作成部と、暗号情報を電子透かしとして画像に合成する電子透かし合成部と、電子透かし合成部によって合成された画像を記録する画像記録部と、電子透かしの抽出方法、暗号情報の復号方法、及び画像識別情報を通知する画像情報通知部とを備えた。



1

【特許請求の範囲】

【請求項１】　画像に電子透かしを合成する電子透かし合成装置であって、
前記画像を入力する画像入力部と、
前記画像を識別する画像識別情報を暗号化した暗号情報を作成する暗号作成部と、
前記暗号情報を電子透かしとして前記画像に合成する電子透かし合成部と、
前記電子透かし合成部によって合成された画像を記録する画像記録部と、
前記電子透かしの抽出方法、前記暗号情報の復号方法、及び前記画像識別情報を通知する画像情報通知部とを備えたことを特徴とする電子透かし合成装置。

【請求項２】　前記暗号作成部は、公開鍵暗号系における秘密鍵に基づいて、前記画像識別情報のデジタル署名を作成することによって、前記暗号情報を作成することを特徴とする請求項１に記載の電子透かし合成装置。

【請求項３】　前記画像識別情報は、前記画像の記録の依頼者毎に異なる識別情報であることを特徴とする請求項２に記載の電子透かし合成装置。

【請求項４】　前記画像識別情報は、前記画像の記録の注文毎に異なる識別情報であることを特徴とする請求項２に記載の電子透かし合成装置。

【請求項５】　前記画像識別情報は、前記画像毎に異なる識別情報であることを特徴とする請求項２に記載の電子透かし合成装置。

【請求項６】　画像の改ざんの有無を判定する画像改ざん判定装置であって、
前記画像を入力する画像入力部と、
前記画像の電子透かし抽出方法、前記電子透かしの暗号を復号する暗号復号方法、及び前記画像を識別する画像識別情報を入力する画像情報入力部と、
前記電子透かし抽出方法に基づいて、前記画像の電子透かしを抽出する電子透かし抽出部と、
前記暗号復号方法に基づいて、前記電子透かしを復号する暗号復号部と、
前記暗号復号部が復号した復号データと、前記画像識別情報とを比較することにより、前記画像の改ざんの有無を判定する改ざん判定部とを備えたことを特徴とする画像改ざん判定装置。

【請求項７】　前記暗号復号部は、前記電子透かしをデジタル署名とみなし、公開鍵暗号系における公開鍵に基づいて前記デジタル署名を復号化することによって、前記復号データを得ることを特徴とする請求項６に記載の画像改ざん判定装置。

【請求項８】　前記画像識別情報は、前記画像の撮影者毎に異なる識別情報又は前記画像毎に異なる識別情報であることを特徴とする請求項７に記載の画像改ざん判定装置。

【請求項９】　画像の改ざんの有無を判定する画像改ざん判定方法であって、

2

前記画像を入力し、
前記画像の電子透かし抽出方法、前記電子透かしの暗号を復号する復号方法、前記画像を識別する識別情報を入力し、
前記電子透かし抽出方法に基づいて、前記画像の電子透かしを抽出し、
前記復号方法に基づいて、前記電子透かしを復号して復号データを抽出し、
前記復号データと、前記画像識別情報とを比較することにより、前記画像の改ざんの有無を判定することを特徴とする画像改ざん判定方法。

【請求項１０】　前記画像の前記識別情報は、前記画像の撮影者毎に異なる識別情報又は前記画像毎に異なる識別情報であることを特徴とする請求項９に記載の画像改ざん判定方法。

【請求項１１】　画像の改ざんの有無を判定するコンピュータ用のプログラムを格納した記録媒体であって、前記プログラムが、
前記コンピュータに前記画像を入力させる画像入力モジュールと、
前記コンピュータに、前記画像の電子透かし抽出方法、前記電子透かしの暗号を復号する復号方法、前記画像を識別する画像識別情報を入力させる画像情報入力モジュールと、
前記電子透かし抽出方法に基づいて、前記画像の電子透かしを抽出させる電子透かし抽出モジュールと、
前記復号方法に基づいて、前記電子透かしを復号化させる暗号復号モジュールと、
前記暗号復号モジュールが復号した復号データと、前記画像識別情報とを比較することにより、前記画像の改ざんの有無を判定させる改ざん判定モジュールとを備えたことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像に電子透かしを合成する画像合成装置及び画像の改ざんの有無を判定する画像改ざん判定装置に関する。

【０００２】

【従来の技術】工事現場において、工事の受注者は、工事の出来高を説明するために、工事の段階ごとに工事現場の写真を撮影し、工事の発注者に提出し、工事が正しく実施されたことを報告する。

【０００３】工事写真をＡＰＳカメラまたはデジタルカメラで撮影した場合、デジタル画像データをＣＤ－ＲＯＭ等の電子媒体で提出することが行われる。しかしデジタル画像データは、コンピュータ等のソフトウエアによって容易にデータを変更することができるため、工事の受注者がデータを改ざんする可能性がある。そのため、工事の発注者が、工事の受注者が提出した画像データに

改ざんがないことを判定する方法が必要である。

【０００４】画像データの改ざんの有無を判定する発明として、特開平１１－９８３４４号公報（公開日１９９９年４月９日）には、予め原画像及びその原画像に埋め込んだ透かし画像を記憶し、改ざんされた可能性のある合成画像を入力した際、合成画像と原画像の差分を検出ことにより、合成画像に埋め込まれた透かし画像を抽出し、予め登録された透かし画像と比較して、改ざんの有無を判定する改ざん判定方法及び装置が開示されている。

【０００５】

【発明が解決しようとする課題】しかしながら、上記の発明においては、改ざん判定装置が、予め原画像を記憶する必要があるため、工事写真のように数多くの画像の改ざんの判定を行わなければならない場合、原画像を記憶するための記憶容量が大きくなるという問題を生じる。

【０００６】そこで本発明は、上記の課題を解決するために、発注者の依頼に基づいて受注者が撮影した画像に電子透かしを合成する画像合成装置、及び受注者が発注者に提出する画像の改ざんの有無を判定する画像改ざん判定装置を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【０００７】

【課題を解決するための手段】上記課題を解決するために、本発明の第１の形態においては、画像に電子透かしを合成する電子透かし合成装置であって、画像を入力する画像入力部と、画像を識別する画像識別情報を暗号化した暗号情報を作成する暗号作成部と、暗号情報を電子透かしとして画像に合成する電子透かし合成部と、電子透かし合成部によって合成された画像を記録する画像記録部と、電子透かしの抽出方法、暗号情報の復号方法、及び画像識別情報を通知する画像情報通知部とを備えたことを特徴とする。

【０００８】暗号作成部は、公開鍵暗号系における秘密鍵に基づいて、画像識別情報のデジタル署名を作成することによって、暗号情報を作成してもよい。

【０００９】画像識別情報は、画像の記録の依頼者毎に異なる識別情報であってもよい。画像識別情報は、画像の記録の注文毎に異なる識別情報であってもよい。画像識別情報は、画像毎に異なる識別情報であってもよい。

【００１０】本発明の第２の形態においては、画像の改ざんの有無を判定する画像改ざん判定装置であって、画像を入力する画像入力部と、画像の電子透かし抽出方法、電子透かしの暗号を復号する暗号復号方法、及び画像を識別する画像識別情報を入力する画像情報入力部と、電子透かし抽出方法に基づいて、画像の電子透かしを抽出する電子透かし抽出部と、暗号復号方法に基づいて、電子透かしを復号する暗号復号部と、暗号復号部が復号した復号データと、画像識別情報とを比較することにより、画像の改ざんの有無を判定する改ざん判定部とを備えたことを特徴とする。

【００１１】暗号復号部は、電子透かしをデジタル署名とみなし、公開鍵暗号系における公開鍵に基づいてデジタル署名を復号化することによって、復号データを得てもよい。

【００１２】画像識別情報は、画像の撮影者毎に異なる識別情報又は画像毎に異なる識別情報であってもよい。

【００１３】本発明の第３の形態においては、画像の改ざんの有無を判定する画像改ざん判定方法であって、画像を入力し、画像の電子透かし抽出方法、電子透かしの暗号を復号する復号方法、画像を識別する識別情報を入力し、電子透かし抽出方法に基づいて、画像の電子透かしを抽出し、復号方法に基づいて、電子透かしを復号して復号データを抽出し、復号データと、画像識別情報とを比較することにより、画像の改ざんの有無を判定することを特徴とする。

【００１４】画像の識別情報は、画像の撮影者毎に異なる識別情報又は画像毎に異なる識別情報であってもよい。

【００１５】画像の改ざんの有無を判定するコンピュータ用のプログラムを格納した記録媒体であって、プログラムが、コンピュータに画像を入力させる画像入力モジュールと、コンピュータに、画像の電子透かし抽出方法、電子透かしの暗号を復号する復号方法、画像を識別する画像識別情報を入力させる画像情報入力モジュールと、電子透かし抽出方法に基づいて、画像の電子透かしを抽出させる電子透かし抽出モジュールと、復号方法に基づいて、電子透かしを復号化させる暗号復号モジュールと、暗号復号モジュールが復号した復号データと、画像識別情報とを比較することにより、画像の改ざんの有無を判定させる改ざん判定モジュールとを備えたことを特徴とする。

【００１６】なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【００１７】

【発明の実施の形態】以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではなく、また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【００１８】以下、本発明を工事写真の例を用いて説明するが、本発明は工事写真に限らず、一般にデジタル画像データに電子透かしを合成し、改ざんの有無を判定することを目的として利用することができる。

【００１９】図１は、本発明の電子透かし合成装置８０と画像改ざん判定装置９０を用いて、工事の受注者が納

品した工事写真のデジタル画像が改ざんされているかどうかを、工事の発注者が判定することのできるシステムの構成図である。

【００２０】電子透かし合成装置８０は、銀塩フィルム、ＡＰＳ（Advanced Photo System）フィルム、デジタルカメラの画像を記録した半導体メモリ等から画像データを読み取り、ＣＤ－ＲＯＭなどの媒体にデジタル化した画像を記録する。通常、電子透かし合成装置８０は、写真の現像サービスを提供するラボシステムにおいて、ラボシステムの従業員が使用する。

【００２１】工事の受注者は、銀塩フィルム、ＡＰＳ（Advanced Photo System）フィルム、半導体メモリ等に記録された、写真の原画像Ｉ０をラボシステムに提供する。ラボシステムの従業員は原画像Ｉ０を電子透かし合成装置８０に入力する。

【００２２】電子透かし合成装置８０は、写真Ｉ０をデジタル化し、写真Ｉ０を識別する画像識別情報に基づいて、暗号情報を作成し、作成された暗号情報を電子透かしとして画像Ｉ０に合成する。電子透かし合成装置８０は合成された画像Ｉ１をＣＤ－ＲＯＭ等に記録して、受注者に提供する。

【００２３】合成画像Ｉ１は、肉眼では原画像Ｉ０と区別がつかないため、受注者が合成画像Ｉ１から電子透かしを検出することは困難である。

【００２４】電子透かし合成装置８０において、画像Ｉ０に合成された電子透かしの抽出方法、電子透かしとして使用された暗号情報の復号方法、及び暗号情報の作成に用いた画像Ｉ０の画像識別情報は、ラボシステムの管理者によって、画像改ざん判定装置９０の使用者、すなわち工事の発注者に通知される。通知手段は、郵便や電子メールなどを用いることができる。

【００２５】受注者は、ラボシステムから合成画像Ｉ１が格納されたＣＤ－ＲＯＭ等の記録媒体を受け取り、ＣＤ－ＲＯＭ等に記録された画像の中から必要な画像を選んで工事の進捗を証明する写真データとして発注者に提出する。発注者に提出された画像は、合成画像Ｉ１に対応する画像Ｉ２であるとし、受注者は画像Ｉ１を改ざんして画像Ｉ２を作成した可能性があるとする。

【００２６】発注者は、受注者が提出した画像Ｉ２に改ざんがあるかどうかを判定するため、画像改ざん判定装置９０を用いる。画像改ざん判定装置９０には予め画像Ｉ１の電子透かし抽出方法と、暗号復号方法と、画像識別情報が入力されている。画像改ざん判定装置９０は画像Ｉ２を入力し、画像Ｉ１の電子透かし抽出方法により、画像Ｉ２の電子透かしを抽出する。抽出した電子透かしを暗号情報とみなし、画像Ｉ１の暗号復号方法により、復号する。さらに、復号されたデータと画像Ｉ１の画像識別情報を比較し、一致するなら画像Ｉ２は画像Ｉ１から改ざんされていないと判定し、一致しないなら画像Ｉ２は画像Ｉ１から改ざんされたと判定する。

【００２７】図２は、本発明の第１の実施形態に係る電子透かし合成装置８０の構成図である。電子透かし合成装置８０は、画像入力部１０と、処理部２０と、記録部４０と、出力部５０とを有する。

【００２８】画像入力部１０は、画像を入力する。銀塩カメラで撮影された画像を画像処理装置に入力する場合、画像入力部１０には、ネガフイルムやポジフイルム等の写真フイルム上の画像を光学的に走査して電気信号に変換するフイルムスキャナが用いられる。デジタルカメラで撮影されたデジタル画像を画像処理装置に入力する場合、画像入力部１０には、入力するデジタル画像を格納した記録媒体に応じた各種読取装置が用いられる。例えば、画像入力部１０には、不揮発性の半導体メモリカード等の着脱自在な記録媒体から画像データを読み取るための読取装置等が用いられる。また、フロッピーディスク、ＭＯ、ＣＤ－ＲＯＭ等から画像データを読み取る場合は、画像入力部１０としてそれぞれフロッピードライブ、ＭＯドライブ、ＣＤドライブ等が用いられる。

【００２９】処理部２０は、暗号情報を作成し、画像入力部１０が入力した画像に暗号情報を電子透かしとして合成する。処理部２０の詳細な構成及び動作は後述する。

【００３０】記録部４０は、処理部２０から受け取った画像を着脱自在な記録媒体に記録する。記録媒体としては、書き込み可能なＣＤ、ＤＶＤ等の光記録媒体や、ＭＯ等の光磁気記録媒体、フロッピー（登録商標）ディスク等の磁気記録媒体等が考えられる。記録部４０としては、ＣＤ－Ｒドライブ、ＤＶＤドライブ、ＭＯドライブ、フロッピードライブ等が用いられる。なお、記録部４０は、半導体メモリ等の記憶装置に画像を記録してもよい。

【００３１】出力部５０は、処理部２０から受け取った画像を出力する。例えば画像を画面表示する場合、出力部５０には画像を表示するモニタが用いられる。

【００３２】次に、処理部２０が作成する暗号情報について説明する。暗号情報の作成には、たとえば公開鍵暗号方式を用いたデジタル署名を用いることができる。

【００３３】公開鍵暗号方式は、暗号鍵と復号鍵が異なり、暗号鍵を公開し、復号鍵を秘密にする。公開された暗号鍵を公開鍵と呼び、秘密にされた復号鍵を秘密鍵と呼ぶ。一方、デジタル署名とは、通信文が改ざんされていないこと及びその通信文の送信者が偽者ではないことを認証する機能である。以下、公開鍵暗号方式を用いたデジタル署名の実現方法を説明する。

【００３４】通信文Ｍに対して、公開鍵ｐｋを用いて暗号化関数Ｅによって暗号化したデータをＥ（Ｍ，ｐｋ）とする。また通信文Ｍに対して、秘密鍵ｓｋを用いて復号化関数Ｄによって復号化したデータをＤ（Ｍ，ｓｋ）とする。

【００３５】公開鍵暗号方式において、公開鍵ｐｋ、暗

号化関数Ｅが与えられたとき、暗号化データＥ（Ｍ，ｐｋ）を求めることは容易である。また秘密鍵ｓｋ、復号化関数Ｄが与えられたとき、復号化データＤ（Ｍ，ｓｋ）を求めることは容易である。

【００３６】公開鍵ｐｋ、暗号化関数Ｅは誰もが知っているため、全ての通信文Ｍに対して、暗号化データＥ（Ｍ，ｐｋ）を容易に計算できるが、秘密鍵ｓｋを知らなければ、暗号化データＥ（Ｍ，ｐｋ）から通信文Ｍを復元することはできない。すなわち、暗号化関数Ｅの逆関数である復号化関数Ｄを求めることは計算量の点で困難である。

【００３７】秘密鍵ｓｋと復号化関数Ｄを知っているなら、暗号化データＥ（Ｍ，ｐｋ）に対して、秘密鍵ｓｋを用いて復元化関数Ｄによって、Ｄ（Ｅ（Ｍ，ｐｋ），ｓｋ）の値を求めることにより、容易に通信文Ｍを復元することができる。すなわち、式

Ｍ＝Ｄ（Ｅ（Ｍ，ｐｋ），ｓｋ）

が成立する。

【００３８】公開鍵暗号方式を用いてデジタル署名を実現するには、公開鍵暗号方式の暗号化、復号化の操作を逆に用いる。公開鍵暗号方式においては、暗号化と復号化を逆に用いて、復号化関数によって通信文を暗号化し、暗号化関数によって暗号化された通信文を復号化することができる。

【００３９】通信文Ｍの送信者は、秘密鍵ｓｋと復号化関数Ｄを知っているとする。送信者通は、通信文Ｍを秘密鍵ｓｋと復号化関数Ｄによって暗号化する。暗号化された通信文はＤ（Ｍ，ｓｋ）である。これを通信文Ｍのデジタル署名と言う。通信文Ｍの送信者は、通信文Ｍとともに、通信文Ｍのデジタル署名Ｄ（Ｍ，ｓｋ）を通信の受信者に送信する。

【００４０】受信者は、公開鍵ｐｋを用いて暗号化関数Ｅによって暗号化データＤ（Ｍ，ｓｋ）を復号化する。復号化されたデータはＥ（Ｄ（Ｍ，ｓｋ），ｐｋ）である。通信の途中で通信文Ｍやデジタル署名Ｄ（Ｍ，ｓｋ）が改ざんされていない限り、復号化されたデータＥ（Ｄ（Ｍ，ｓｋ），ｐｋ）の値はＭに一致する。すなわち式

Ｍ＝Ｅ（Ｄ（Ｍ，ｓｋ），ｐｋ）

が成立する。

【００４１】仮に、通信文ＭがＭ＊に改ざんされたとすれば、デジタル署名を復号化したデータＥ（Ｄ（Ｍ，ｓｋ），ｐｋ）はＭになるが、受信した通信文はＭ＊である。すなわち、式

Ｍ＊≠Ｍ＝Ｅ（Ｄ（Ｍ，ｓｋ＊），ｐｋ）

が成立する。したがって、デジタル署名の復号結果と受信した通信文が異なることから、通信文が改ざんされたことを知ることできる。

【００４２】ここで、Ｄ（Ｍ，ｓｋ）の計算ができるのは、秘密鍵ｓｋを知っているのは通信文の送信者本人だけである。したがって、第３者が通信文ＭをＭ＊に改ざんした後に、通信文Ｍ＊に対するデジタル署名Ｄ（Ｍ＊，ｓｋ）を作成することは不可能である。すなわち、通信文Ｍを改ざんするとともに、それに合わせてデジタル署名を改ざんして、改ざんを隠蔽することはできない。

【００４３】また、通信の受信者と同じ公開鍵暗号系で通信を行う他人が、通信文Ｍの送信者になりすまして、デジタル署名を作成することはできない。なぜなら、秘密鍵ｓｋは通信部Ｍの送信者しか知らないため、他人が通信文Ｍのデジタル署名Ｄ（Ｍ，ｓｋ）を作成することはできないからである。仮に、他人が異なる秘密鍵ｓｋ＊と復号化関数Ｄを用いて求めた、通信文Ｍのデジタル署名Ｄ（Ｍ，ｓｋ＊）を通信文Ｍとともに通信の相手に送ると、通信の受信者は、デジタル署名Ｄ（Ｍ，ｓｋ＊）を試みる。復元された通信文はＥ（Ｄ（Ｍ，ｓｋ＊），ｐｋ）であるが、これは通信文Ｍには一致しない。すなわち、式

Ｍ≠Ｅ（Ｄ（Ｍ，ｓｋ＊），ｐｋ）

が成立する。したがって、他人が通信文Ｍの送信者になりすまして、通信文Ｍを送信したことを検出することができる。

【００４４】以上述べたように、公開鍵暗号方式を用いることにより、デジタル署名を実現できる。すなわち通信文の改ざんがなされていないこと、他人が通信文の真の送信者になりすまして通信文を送信していないことを認証することができる。尚、公開鍵暗号、デジタル署名については、「暗号理論入門」（岡本栄司著、共立出版）に詳しい。

【００４５】本実施形態の電子透かし合成装置８０では、上述の通信文Ｍとして、画像識別情報ＩＤを用い、画像識別情報ＩＤのデジタル署名を作成し、電子透かしとして画像に合成する。

【００４６】画像識別情報ＩＤは、たとえば受注者を識別する受注者識別情報、受注者がラボシステムに画像のデジタル化を依頼したときの注文を識別する注文識別情報、画像入力部１０が入力した画像を識別する画像毎の識別情報のいずれであってもよい。

【００４７】図３は、本実施形態の電子透かし合成装置８０の処理部２０の機能ブロック図である。処理部２０は、暗号作成部２２と、電子透かし合成部２４と、画像情報通知部２６とを有する。

【００４８】暗号作成部２２は、公開鍵暗号系の秘密鍵及び画像識別情報ＩＤを用いて、暗号情報の一例としてデジタル署名を作成する。当該電子透かし合成装置８０を使用するラボシステムの管理者と工事の発注者の間では公開鍵暗号が用いられ、秘密鍵は、ラボシステムの管理者が秘匿し、公開鍵は発注者に知らされる。

【００４９】電子透かし合成部２４は、暗号作成部２２が作成したデジタル署名を電子透かしとして画像入力部

１０が入力した画像に合成する。

【００５０】画像識別情報ＩＤが、受注者識別情報である場合、同一の受注者であれば、画像入力部１０が入力した画像のすべてに同一のデジタル署名が作成され、電子透かしとして埋め込まれる。

【００５１】画像識別情報ＩＤが、注文識別情報である場合、同一の受注者であっても、注文単位毎に異なるデジタル署名が作成され、電子透かしとして埋め込まれる。

【００５２】画像識別情報ＩＤが、画像毎に異なる識別情報である場合、画像入力部１０が入力した画像毎に異なるデジタル署名が作成され、電子透かしとして埋め込まれる。

【００５３】画像毎に異なる画像識別情報ＩＤの例としては、たとえば、ランダムに生成した画像のファイル名であってもよい。また、画像データの一部分を取り出して、画像識別情報ＩＤとしてもよい。また、画像データの色情報、明度、彩度に関する情報など、画像毎に異なる情報を画像識別情報ＩＤとしてもよい。

【００５４】画像情報通知部２６は、暗号作成部２２が作成したデジタル署名の復号化方法、電子透かし合成部２４が合成した電子透かしの抽出方法、及び暗号作成部２２がデジタル署名を作成するときに用いた画像識別情報ＩＤを、工事の発注者又は画像改ざん判定装置９０に通知する。通知手段として電子メールや郵便等を用いることができる。

【００５５】図４は、電子透かし合成方法のフローチャートである。本図を参照しながら、電子透かし合成装置８０が行う電子透かし合成方法を説明する。

【００５６】画像入力部１０は画像を入力する（Ｓ２００）。暗号作成部２２は、画像識別情報ＩＤに対して、秘密鍵ｓｋ及び復号化関数Ｄを用いてデジタル署名Ｄ（ＩＤ，ｓｋ）を作成する（Ｓ２０２）。

【００５７】電子透かし合成部２４は、暗号作成部２２が作成したデジタル署名を電子透かしとして画像入力部１０が入力した画像に合成する（Ｓ２０４）。電子透かしを画像に合成する方法及び合成された電子透かしを画像から抽出する方法は、「電子透かしの基礎～マルチメディアのニュープロテクト技術～」（松井甲子雄著、森北出版）に記載された方法を用いることができる。

【００５８】記録部４０は、電子透かし合成部２４が合成した画像をＣＤ－ＲＯＭなどの記録媒体に記録する（Ｓ２０６）。

【００５９】電子透かし合成装置８０を用いて合成された画像は、記録部４０によってＣＤ－ＲＯＭなどに格納されて受注者に渡される。

【００６０】受注者はＣＤ－ＲＯＭに格納された画像を選択して、工事を説明する写真データとして発注者に提出する。発注者は、受注者が提出した画像から電子透かしを抽出し、抽出された電子透かしをデジタル署名の復号化方法にしたがって、復号化する。電子透かしがデジタル署名Ｄ（ＩＤ，ｓｋ）であるとき、復号されたデータは、Ｅ（Ｄ（ＩＤ，ｓｋ）、ｐｋ）である。Ｅ（Ｄ（ＩＤ，ｓｋ）、ｐｋ）が、先にラボシステムから通知された画像識別情報ＩＤに等しいかどうかを調べ、改ざんの有無を検出する。

【００６１】受注者は画像に埋め込まれた電子透かしを見破ることは困難である。仮に受注者が画像データを改ざんした場合、画像に埋め込まれた電子透かしの情報が壊れる。そのため、発注者が改ざんされた画像データから電子透かし情報を抽出し、デジタル署名を取り出し、デジタル署名を復号化しても画像識別情報ＩＤが正しく復元されない。したがって発注者は、ラボシステムの管理者から通知された画像識別情報と比較して、画像データが改ざんされたことを知ることができる。

【００６２】仮に受注者がデジタル署名の作成に使用した画像識別情報ＩＤを知っても、公開鍵暗号系を用いたデジタル署名の場合、秘密鍵を知らない限りはデジタル署名を作成することができない。したがって、受注者が自ら画像識別情報ＩＤからデジタル署名を作成して、画像に電子透かしとして埋め込むことはできない。

【００６３】画像識別情報ＩＤとして、受注者識別情報を使用した場合、受注者毎にデジタル署名が同じになる。画像識別情報ＩＤとして、注文識別情報を使用した場合、同一の受注者であっても、注文単位毎にデジタル署名が変わる。そのため、受注者が電子透かしとして埋め込まれたデジタル署名を見破ることは困難になる。

【００６４】画像識別情報ＩＤとして、画像データ毎に異なる識別情報を用いた場合、デジタル署名は画像毎に一つ一つ異なるため、受注者が電子透かしとして画像に埋め込まれたデジタル署名を見破ることは一層困難になり、改ざんを防止する効果を高めることができる。

【００６５】図５は、本発明の第２の実施形態に係る画像改ざん判定装置９０の構成図である。画像改ざん判定装置９０は、画像入力部１１と、画像情報入力部１２と、処理部６０と、出力部５０とを有する。

【００６６】画像入力部１１は、記録媒体に格納された画像を入力する。フロッピーディスク、ＭＯ、ＣＤ－ＲＯＭ等から画像データを読み取る場合は、画像入力部１０としてそれぞれフロッピードライブ、ＭＯドライブ、ＣＤドライブ等が用いられる。

【００６７】画像情報入力部１２は、画像入力部１１が入力する画像に関して、電子透かしを抽出する方法、暗号号情報の復号方法の一例として、デジタル署名の暗号を復号する方法、及び画像識別情報ＩＤを入力する。

【００６８】処理部６０は、画像入力部１０が入力する画像の電子透かしを抽出し、抽出した電子透かしをデジタル署名として、デジタル署名を復号化し、画像識別情報を抽出し、改ざんの有無を判定する。

【００６９】出力部５０は、処理部２０から受け取った

画像を出力する。例えば画像を画面表示する場合、出力部５０には画像を表示するモニタが用いられる。

【００７０】図６は、処理部６０の機能ブロック図である。処理部６０は、電子透かし抽出部６２と、暗号復号部６４と、改ざん判定部６６とを有する。

【００７１】電子透かし抽出部６２は、画像情報入力部１２が入力した電子透かし抽出方法を用いて、画像入力部１０が入力した画像から電子透かしを抽出する。暗号復号部６４は、抽出された電子透かしをデジタル署名とみなし、画像情報入力部１２が入力したデジタル署名の復号方法を用いて、デジタル署名を復号化する。改ざん判定部６６は、暗号復号部６４が復号化して得られたデータと、画像情報入力部１２が入力する画像識別情報ＩＤとが一致するかどうかを検出することにより、改ざんの有無を判定する。

【００７２】図７は、画像改ざん判定方法のフローチャートである。本図を参照しながら、画像改ざん判定装置９０が行う画像改ざん判定方法を説明する。

【００７３】画像入力部１１は画像を入力する（Ｓ２２０）。画像情報入力部１２が、画像入力部１０が入力した画像に関する、電子透かし抽出方法、デジタル署名復号方法及び画像識別情報ＩＤを入力する（Ｓ２２２）。

【００７４】電子透かし抽出部６２は、画像情報入力部１２が入力した電子透かし抽出方法に基づいて画像から電子透かしを抽出する（Ｓ２２４）。暗号復号部６４は、電子透かし抽出部６２が抽出した電子透かしをデジタル署名Ｄ（ＩＤ，ｓｋ）の値であるとみなし、公開鍵ｐｋを用いて復号化する。暗号復号部６４は、画像情報入力部１２が入力する復号方法から暗号化関数Ｅを知り、公開鍵ｐｋを用いて暗号化関数Ｅにより、デジタル署名Ｄ（ＩＤ，ｓｋ）を復号化し、復号化データとしてＥ（Ｄ（ＩＤ，ｓｋ）、ｐｋ）を得る（Ｓ２２６）。

【００７５】改ざん判定部６６は、暗号復号部６４が復号化したデータＥ（Ｄ（ＩＤ，ｓｋ）、ｐｋ）が、画像情報入力部１２が入力する画像識別情報ＩＤに等しいかどうかを調べる（Ｓ２２８）。もし等しいなら、画像は改ざんされていないと判定し（Ｓ２３０）、もし等しくないなら、画像は改ざんされていると判定する（Ｓ２３２）。

【００７６】本実施形態の画像改ざん検出装置によれば、受注者が発注者に提出する画像から電子透かしを抽出し、電子透かしをデジタル署名とみなし、復号化することによって画像識別情報を取り出すことができる。得られた画像識別情報を、先にラボシステムの管理者から通知された画像識別情報と照合することにより、画像の改ざんの有無を検出することができる。

【００７７】図８は、本発明の第３の実施形態に係る画像改ざん判定装置の構成図である。本実施形態の画像改ざん判定装置の基本的な構成及び動作は、図５で示した第２の実施形態の画像改ざん判定装置と同様である。本実施形態では、画像改ざん判定装置の処理部６０として、パーソナルコンピュータやワークステーション等の電子計算機を用いる点が、第２の実施形態と異なる。

【００７８】図８を参照しながら、処理部６０のハードウエア構成を説明する。ＣＰＵ３０はＲＯＭ３２及びＲＡＭ３４に格納されたプログラムに基づいて動作する。キーボード、マウス等の入力装置３１を介して利用者によりデータが入力される。ハードディスク３３は、画像等のデータ、及びＣＰＵ３０を動作させるプログラムを格納する。ＣＤ－ＲＯＭドライブ３５はＣＤ－ＲＯＭ１００からデータ又はプログラムを読み取り、ＲＡＭ３４、ハードディスク３３及びＣＰＵ３０の少なくともいずれかに提供する。

【００７９】処理部６０のＣＰＵ３０が実行するソフトウエアの機能構成は、図６と同じであり、電子透かし検出モジュール１６２と、暗号復号モジュール１６４と、改ざん判定モジュール１６６とを有する。

【００８０】電子透かし検出モジュール１６２、暗号復号モジュール１６４、及び改ざん判定モジュール１６６がコンピュータに働きかけて、ＣＰＵ３０に行わせる処理は、それぞれ図６に示した、第２の実施形態の画像改ざん判定装置９０における、電子透かし抽出部６２、暗号復号部６４、及び改ざん判定部６６の機能及び動作と同一であるから、説明を省略する。これらのソフトウエアは、ＣＤ－ＲＯＭ１００等の記録媒体に格納されて利用者に提供される。ソフトウエアは記録媒体からハードディスク３３にインストールされ、ＲＡＭ３４に読み出されてＣＰＵ３０により実行される。

【００８１】記録媒体の一例としてのＣＤ－ＲＯＭ１００には、本出願で説明した処理部２０又は処理部６０の動作の一部又は全ての機能を格納することができる。またＣＤ－ＲＯＭ１００には他の装置の動作の一部又は全ての機能を格納することができる。これらのプログラムは記録媒体から直接ＲＡＭ３４に読み出されて実行されてもよい。

【００８２】記録媒体としては、ＣＤ－ＲＯＭ１００の他にも、ＤＶＤやＰＤ等の光学記録媒体、フロッピーディスクやミニディスク（ＭＤ）等の磁気記録媒体、ＭＯ等の光磁気記録媒体、テープ状記録媒体、不揮発性の半導体メモリカード等を用いることができる。上記のプログラムを格納した記録媒体は、電子透かし合成装置及び画像改ざん判定装置を製造するためにのみ使用されるものであり、そのような記録媒体の業としての製造および販売等が本出願に基づく特許権の侵害を構成することは明らかである。

【００８３】以上述べたように、第１の実施形態の電子透かし合成装置によれば、受注者の写真の画像データに対して、画像識別情報に対するデジタル署名を作成し、電子透かしとして画像に合成することができる。

【００８４】受注者が画像の改ざんを行うと、電子透か

しの情報が壊れるため、改ざんの形跡を画像に残すことができる。合成された電子透かしは受注者が容易に取り出すことができない。仮に電子透かしが抽出されたとしても、抽出された電子透かしは画像識別情報のデジタル署名であり、容易に復号化することができない。

【００８５】画像識別情報として、受注者毎に異なる情報、注文毎に異なる情報、及び画像毎に異なる情報を使い分けることにより、電子透かしとして埋め込まれたデジタル署名のセキュリティの強さを変えて、改ざんの防止の効果を向上させることができる。

【００８６】第２の実施形態の画像改ざん検出装置によれば、受注者が発注者に提出する画像から電子透かしを抽出し、電子透かしをデジタル署名とみなし、復号化することによって画像識別情報を取り出すことができる。得られた画像識別情報は、先にラボシステムの管理者から通知された画像識別情報と照合され、画像の改ざんの有無を検出することができる。

【００８７】以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることができることが当業者に明らかである。その様な変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【００８８】

【発明の効果】上記説明から明らかなように、本発明によれば、発注者の依頼に基づいて受注者が撮影した画像に電子透かしを合成し、受注者が発注者に提出する画像の改ざんの有無を判定することができる。

【図面の簡単な説明】

【図１】　本発明の電子透かし合成装置８０と画像改ざん判定装置９０を用いて、画像の改ざんの有無を判定するシステムの構成図である。

【図２】　本発明の第１の実施形態に係る電子透かし合成装置８０の構成図である。

【図３】　処理部２０の機能ブロック図である。

【図４】　電子透かし合成方法のフローチャートである。

【図５】　本発明の第２の実施形態に係る画像改ざん判定装置９０の構成図である。

【図６】　処理部６０の機能ブロック図である。

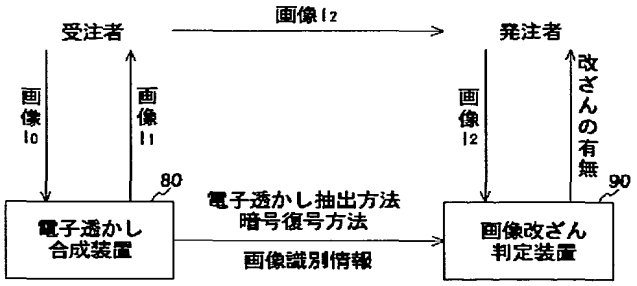
【図７】　画像改ざん判定方法のフローチャートである。

【図８】　本発明の第３の実施形態に係る画像改ざん判定装置の構成図である。

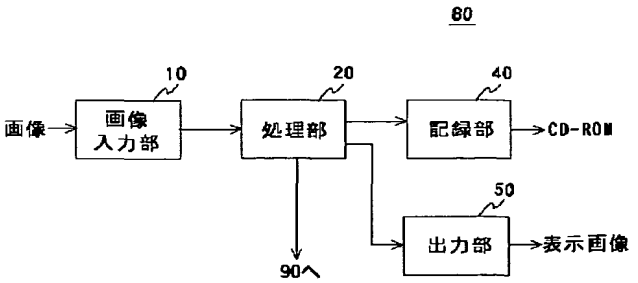
【符号の説明】

１０	画像入力部	１２	画像情報入力部
２０	処理部	２２	暗号作成部
２４	電子透かし合成部	２６	画像情報通知部２６
４０	記録部	５０	出力部
６０	処理部	６２	電子透かし抽出部
６４	暗号復号部	６６	改ざん判定部
８０	電子透かし合成装置	９０	画像改ざん判定装置

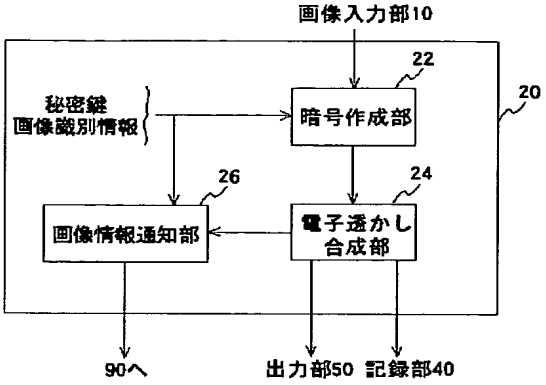
【図１】



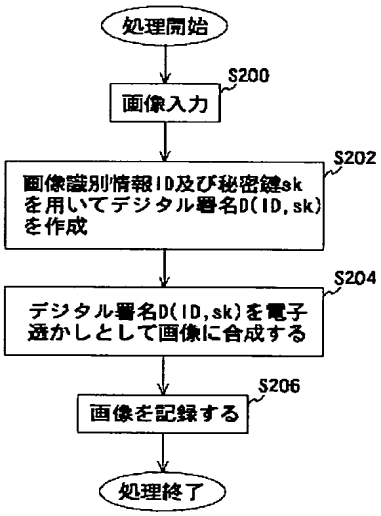
【図２】



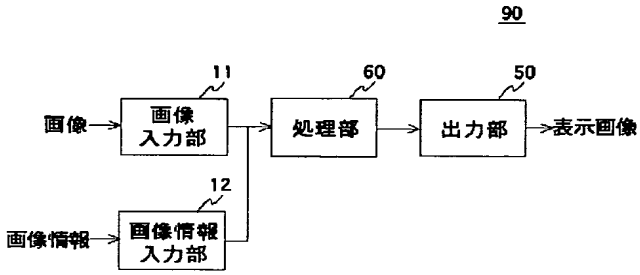
【図３】


画像入力部10
22
秘密鍵
画像識別情報
暗号作成部
20
26
24
画像情報通知部
電子透かし
合成部
90へ
出力部50
記録部40

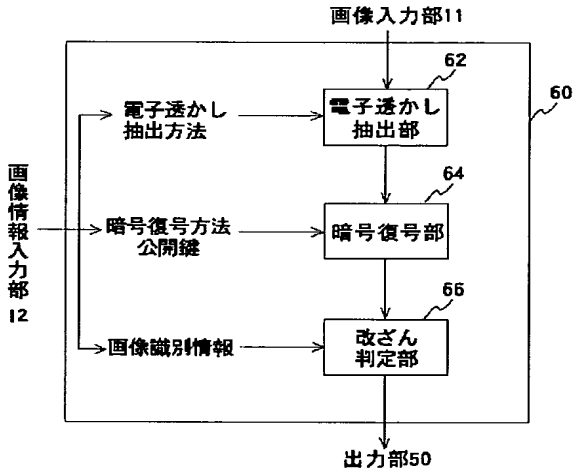
【図４】


処理開始
S200
画像入力
S202
画像識別情報ID及び秘密鍵sk
を用いてデジタル署名D(ID,sk)
を作成
S204
デジタル署名D(ID,sk)を電子
透かしとして画像に合成する
S206
画像を記録する
処理終了

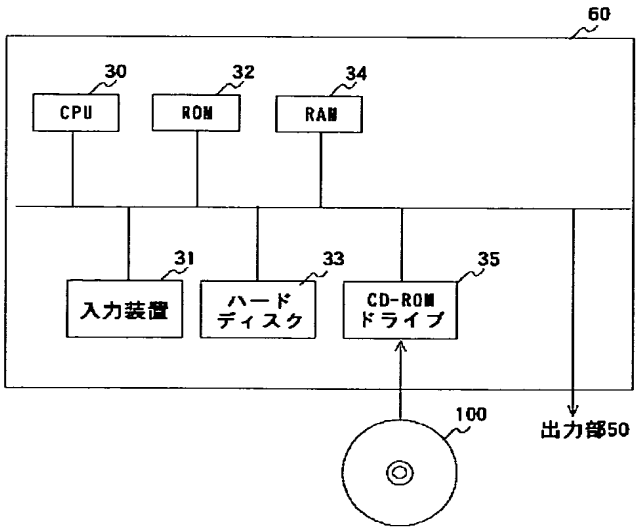
【図５】


90
11
60
50
画像
画像
入力部
処理部
出力部
表示画像
12
画像情報
画像情報
入力部

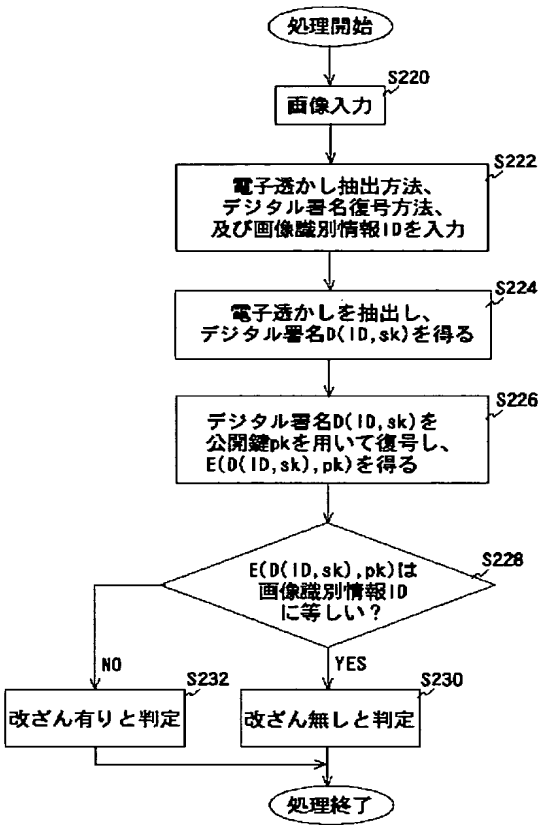
【図６】


画像入力部11
62
60
電子透かし
抽出方法
電子透かし
抽出部
64
画像
情報
入力部
12
暗号復号方法
公開鍵
暗号復号部
66
画像識別情報
改ざん
判定部
出力部50

【図８】


60
30
32
34
CPU
ROM
RAM
31
33
35
入力装置
ハード
ディスク
CD-ROM
ドライブ
100
出力部50

【図７】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３Ｅ

Ｆターム(参考)　5B057 AA20 CE08
5C076 AA14 BA06
5J104 AA07 AA09 AA14 KA01 KA05
LA03 LA06 NA02 NA05 NA29
NA32 PA14